An Internet of Things and Blockchain Based Smart Campus Architecture

Manal Alkhammash[1,2], Natalia Beloff[2] , and Martin White[2]

[1] Jazan University, Jazan, KSA
[2] Sussex University, Brighton, UK
{ma979,n.beloff,w.white}@sussex.ac.uk

Abstract. Rapid development in science and information technologies, such as the Internet of things, has led to a growth in the number of studies and research papers on smart cities in recent years and more specifically on the construction of smart campus technologies. This paper will review the concept of a smart campus, discuss the main technologies deployed, and then propose a new novel framework for a smart campus. The architecture of this new smart campus approach will be discussed with particular consideration of security and privacy systems, the Internet of things, and blockchain technologies.

Keywords: Smart campus, Internet of things, Blockchain, Security, Privacy.

1 Introduction

Information and communications technology (ICT) development is a never-ending process, which has led to a growth in the number of studies and research papers on smart cities in recent years. The concept of a smart city is not only about constructing traditional infrastructure, such as a transportation system, but also involves ICT infrastructure in order to improve quality of life and enhance the profile of the city [1]. Therefore, the term ‘smart city’ can be generally defined as dynamically integrating the physical and the digital worlds, in which different data resources are automatically gathered in real time [1–3]. By utilising high-speed networks, the changes in the physical world can be captured and transferred to data centres so that they can be stored and processed [4]. This means that in order to capture the necessary data, there needs to be significant numbers of sensors at diverse locations that can capture this ‘big data’. In addition, the Cloud needs to be utilised in order to store and analyse the data.

Consequently, there are many areas that can be developed under the intelligent city framework to achieve the overall goal of improving citizens’ quality of life. There have been many contributions and research papers in different areas to develop smart systems, such as medical and health care [5–8], supply chain management [9, 10], traffic [11, 12], and education systems [13–15] that together can build smart cities.

Since a smart campus constitutes an essential element of a smart city, and the concept of the smart campus comes from the notion of smart cities [16], many researchers have focused their attention on developing smart campuses, trying to address the topical question of ‘how to develop an intelligent campus’ by contributing the same ideas and bases of intelligent cities to propose the smart campus [17]. Therefore, the aim of this paper is to study different technologies and to design a novel architecture for a smart campus in order to develop an intelligent campus. Such a smart and intelligent campus architecture (or framework) is likely to exploit the Internet of things (IoT), blockchain, and smart contracts as part of its many technology solutions.

The paper will be structured as follows. In section two a brief description of a smart campus concept will be addressed. In section three the paper provides a brief background of a smart campus and delineates the main areas of the campus. In section four the paper reports some issues related to a previous generic smart campus architecture and proposes a new one and discusses it in depth in the following section. Finally, in section six the paper provides conclusions and future work.

2 Smart Campus Concept

Traditionally, a campus can be defined as a land or an area where different buildings constitute an educational establishment. A campus often includes classrooms, libraries, student centres, residence halls, dining halls, parking, etc. Nowadays, campuses have adopted advanced technologies, such as visual learning environments [18, 19] and timetabling systems [20, 21] in order to provide high-quality services for stakeholders (e.g. academics, students, administrators, and services functions) on campus and to monitor and control facilities. These developments should be evolving constantly in order to increase efficiency, cut operational costs, reduce effort, lead to better decision-making, and enhance the student experience [22]. Thus, the term 'smart campus' can be defined as a place where digital infrastructure can be developed and that has the ability to gather information, analyse data, make decisions, and respond to changes occurring on campus without human intervention [22, 23]. The authors in [24] define a smart campus as an environment where the structure of ambient learning spaces – application context based on virtual spaces – integrates social and digital services into physical learning resources.

If we think of a smart campus as a holistic framework, it encompasses several themes, including but not limited to automated security surveillance and control, intelligent sensor management systems, smart building management, communication for work, cooperation and social networking, and healthcare. Several innovations have been proposed for smart campuses, ranging from developing a whole framework using technologies such as mobile technologies, blockchain, the IoT, and the Cloud to assist learning to enhancing security systems utilising technologies such as ZigBee and radio frequency identification (RFID) [25–28].

3 Smart Campus Background

Many studies and architectural plans with different goals have been undertaken on the subject of the smart campus [29]. This smart campus research largely breaks down into the following areas: teaching and learning, data analysis and services, building management and energy use on campus, campus data mining, water and waste management use on campus, campus transportation, and campus security.

3.1 S mart Campus Leaning Environments

Much research has been focused on constructing smart campuses by developing suitable technologies and applications that involve teaching and learning. Therefore, the common purpose of designing and developing a smart campus has often been from a learning and educational perspective. The authors in [27] developed a novel holistic environment for a smart campus known as iCampus. The aim of their research is to propose a beginning-to-end lifecycle within the knowledge ecosystem in order to enhance learning. Atif and Mathew designed a framework for a smart campus that integrates a campus social network within a real-world educational facility [30]. The study's goal was to provide a social community where knowledge could be shared between students, teachers, and the campus's physical resources. Further, [1] proposed a model of a smart campus to enable stakeholders on the campus to shape and understand their learning futures within the learning ecosystem. Based on cloud computing and IoT, [31] stated the concept of a smart campus and demonstrated some issues that related to intelligence application platforms after establishment. However, these approaches were focused only on proposing a smart campus by using IoT technology.

3.2 S mart Campus Data Analysis and Service Orientation

Other research has considered the development of smart campuses based on data analysis. According to [32], a smart campus should be able to gather data from a crowd and analyse it by using crowdsourcing technologies in order to deliver services of added value. In 2011, [33] explained the prototype of a smart campus implementation that uses semantic technologies in order to integrate heterogeneous data. However, some researchers have envisioned smart campuses from social networking aspects. For instance, [34] elaborated upon an architectural system that can be deployed on campus in order to support social interaction by using service-oriented specifications. This will depend upon their proposed social network platform (WeChat) and an examination of its architecture, functions, and features. Xiang et al. developed a smart campus framework based on information dissemination [17]. However, these approaches did not address blockchain technology in order to eliminate centralisation.

3.3 Building Management and Energy Efficiency on Smart Campuses

Several of the current initiatives that are developing smart campuses have been based on high-energy efficiency perspectives. In order to decrease the energy consumption of buildings, monitoring and controlling environmental conditions is essential, such as controlling both natural and artificial lighting, humidity, and temperature. An example of this is a project that was undertaken at the University of Brescia in Italy in 2015 that aimed to enhance energy efficiency inside buildings by monitoring lighting, temperature, and electrical equipment by using control systems, automation, and grid management. The project progressed in stages towards this goal. First of all, it aimed to reduce the consumption of the buildings' energy by analysing possible actions.

Then it attempted to implement different measures and evaluated their efficiency. Simultaneously, in order to enhance users' awareness of energy consumption, a system for monitoring operational conditions was also developed. Finally, the project evaluated the energy balance between consumption and generation, renewable energy production, and energy reduction. The outcome displayed a significant energy consumption reduction of 37.3% while improving the buildings' thermal properties [35].

In addition, [36] proposed and implemented a web-based system to manage energy in campus buildings known as CAMP-IT. The system aimed to optimise the operation of energy systems in order for buildings to achieve goals of reducing energy consumption while at the same time enhance the quality of the indoor environment in terms of visual comfort and air quality. The modelling collected, controlled, and analysed the energy load for each building and for the campus as a whole. The results showed a reduction in energy consumption of nearly 30%. Again, these approaches did not study the integration of blockchain into the proposed architectures.

3.4 Smart Campus Data Mining

Additionally, some researchers have focused on applying interest mining, which is based on location, context awareness, proximity, and user profiles as well as other related information, to assist users in meeting their needs within the campus environment. In 2014, [37] studied web log mining, which is an essential technique in web data mining to determine users' characteristic interests by developing a reliable and efficient method of data pre-processing. In 2010, [38] proposed a data-mining method from e-learning systems to identify users' interests and obtain information about learners' logs and knowledge background. Along these lines, the model would be able to automatically recommend resources that may be of interest to individual students. However, blockchain technology could be used to protect user profiles and preferences.

3.5 Water Management on Smart Campuses

Regarding water and waste management, since they are considered expensive and important services on smart campuses, several research studies have focused on proposing management systems on campuses for these services in order to reduce the environmental and financial impact [22]. In terms of sustainable water management, there are three important pillars: water harvesting processes, water recycling, and water consumption reduction [39].

Different approaches have been proposed to manage water. Some focused on controlling and monitoring the water level and water consumption on campus. For instance, [40] developed a water monitoring system to reduce water consumption on campus. The system designed a three-dimensional map of the campus and used a geographical information system (GIS) to display a water pipeline in the electronic map with detailed status information in real time. Therefore, the model can monitor water directly from pipelines; detect any problems that occur in the equipment, such as leaking; and analyse the amount of water consumption.

In 2015, [41] developed a suitable system for medium-sized campuses to monitor the water balance in real time. The design used an ultrasound level sensor, a cloud software stack, and communication links and carefully considered industrial design.

To be able to monitor the water, the system measured the water level in tanks by sending ultrasound pulses to the water's surface. After observing the reflection, the sensors can estimate the distance and calculate the tank volume. Based on previous work, [42] developed an automatic water distribution system for large campuses so that each tank on the campus would have enough water to meet the local needs. The authors utilised ultrasonic ranging sensors, which are suitable for measuring water levels in large tanks, and a wireless network using sub-GHz radio frequency to connect sensors across long distances for further analysis.

Moreover, many other experiments have proved efficient for developing water management systems, and they can be implemented on smart campuses to reduce water consumption [43]. For example, [44] developed a meter of a smart water that can provide a user with real-time reading information, analyse his consumption data, and present it in visual graphs to improve the readability. Simultaneously, the system monitors the consumption and alerts the user if there is unusual water usage. However, these approaches did not address blockchain technology.

3.6 Waste Management on Smart Campuses

Similarly, numerous studies have been devoted to developing waste management systems. Authors in [45, 46] stated that general research studies in this area focused on developing waste tracks and bins with sensor devices attached to collect and analyse real-time data. This information can be used for several purposes, for example, for developing an efficient cleaning timetable and preventing overfilling of bins. Ebrahimi et al. [47] in 2017 investigated the current waste and recycling infrastructure on Western Kentucky University campus to determine whether it had an adequate service by using spatial techniques, such as GIS, to track, recognise, and visualise waste and recycling bins in a large-scale area. They used spatial information for analysis and decision making to reduce solid waste steam and improve the university's recycling stream. Furthermore, they drew an accurate roadmap for a suitable waste management plan for the campus. Although most papers use different techniques for waste management systems on smart campuses, they are still at the primary stages, and they lack a generic model.

3.7 Smart Campus Transportation

Recently, global positioning system (GPS) has become the most common method for streaming a location and tracking a moving object, such as a vehicle on the road. To improve the accuracy of GPS, external information is needed, such as Wi-Fi, digital imaging, and computer vision [48]. The authors in [49] developed a tracking system for buses using GPS devices that reported the buses' locations every ten seconds. The location was sent from the server via SMS. The system also had safety features, such as the ability to send alerts or emergency reports when the vehicle crashed or was stolen. Other studies have tracked the location of a college bus using a mobile phone and Google Maps [50, 51]. Saad et al. [48] developed a real-time monitoring system for a university bus that used a GPS service to send the location of the bus to a cloud database every second. The system could also analyse data to estimate the bus's arrival time. However, these approaches did not use blockchain technology to improve system security.

3.8 Smart Campus Security

Many mobile applications have been developed for campus safety. Some of them allow users to contact campus security guards, such as EmergenSee and CampusSafe, whereas others, such as Guardly and CircleOf6, allow friends to contact each other [52]. These applications allow user location, photos, and situation descriptions to be shared with campus security guards.

In addition, [53] also proposed a smart campus framework that includes several aspects, of which security was a notable one. They pointed out that a smart system can reduce burglaries by detecting glass breaking or any distinct sound; then, the system has the ability to alert security to the location. Also, the system may have the ability to reduce drug or alcohol abuse by alerting public safety to the presence of alcohol.

Therefore, a smart campus can be described as an environment that has the ability to provide a suitable infrastructure in order to deliver services required in light of contextual awareness. In addition, it is a well-structured place that can generate huge amounts of information to a number of users by using their profiles and locations in order to best address their needs. Consequently, the desirable characteristics of a smart campus are accurate context awareness and ubiquitous access to networks, efficient and optimal utilisation, many varied resources, and the use of objective principles as a basis to make smart decisions or predictions.

3.9 Summary

All the above approaches and implementations are useful and contribute to building smart campuses; however, they rely on IoT technologies with a centralised system architecture, which could lead to many issues and will be discussed in the next section. Next, we describe a new architecture that incorporates a distributed architecture exploiting blockchain and smart contracts to overcome some of the prevalent issues.

4 Smart Campus Concept

Developing an architecture for a smart campus while considering advanced technologies, such as IoT, blockchain, and other technologies, is a complicated and difficult task since there are a large variety of devices and objects, associated services with such a system, and link layer technologies.

Many different smart campus architectures have been developed with different aims [22, 29]. However, most of these frameworks usually contain three essential layers that interact with each other. First is the perception layer, which contains physical technologies, such as sensors, that collect all kinds of data from the surrounding environment. Second is the network layer, which contains all communication networks that are responsible for receiving and transmitting data. Third is the application layer, which is responsible for supporting business and personalised services and interacting with individual users. Figure 1 shows a generic illustration of this layered architecture approach.

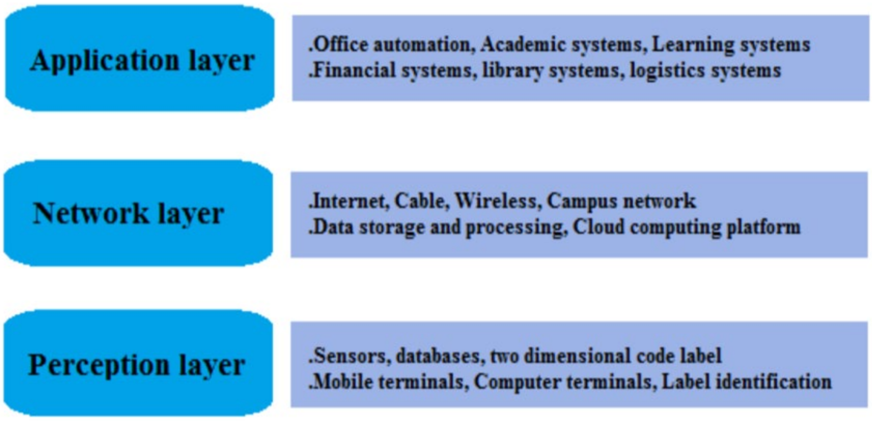

Fig. 1. A generic smart campus layered architecture [54]

Here, we can see on the lowest level of the architecture that the perception layer is allocated, and it accommodates sensors to extract and gather the data from physical devices. In the middle of the architecture the network layer is utilised to aggregate, filter, and transmit data. The last layer is used by the Cloud or servers to store and analyse smart campus data.

There are several problems with this generic architecture since it relies on IoT architecture. The IoT systems rely on centralised computing and storage platforms, such as cloud platforms, which is a suitable place to start for joining, managing, and controlling a massive number of different objects and devices as well as providing the required authentication and identification for various IoT devices. However, the centralised system architecture suffers from several limitations. Atlam and Wills [55] studied these limitations as follows. First, the centralised system has privacy vulnerabilities because data is collected from different devices and then stored in a centralised platform, which can be easily breached. Second, security is a major aspect for any system since processing and storing data through a centralised platform can lead to it being an easy target for attacks, such as distributed denial of service (DDoS) and denial of service (DoS) attacks. In addition, the devices in the IoT system are heterogeneously connected in nature, while a centralised platform uses a single operating system to connect to various devices. In this case, a centralised platform could prevent some objects from connecting to the system. Lastly, scalability is another issue related to a centralised platform since the number of connecting devices in the system is increasing. This is especially a problem for large business organisations, such as campuses, that are distributed in different areas. According to Piekarska and Halpin [56], there are concerns about the efficiency of operating and the scale of the IoT system with centralised architecture taking into account the increasing demands.

Recently, blockchain technology has been involved in various application areas beyond the cryptocurrency domain since it has multiple features, such as decentralisation, support for integrity, resiliency, autonomous control, and anonymity [57]. Blockchain eliminates a central authority by using a distributed ledger and is decentralised to provide more efficiency for operating and controlling communication among all participating nodes. It also eliminates the single point of failure if the centralised platform goes down, which could lead to the failure of a whole system [55]. Therefore, blockchain can be an efficient technology to handle the issues related to a centralised IoT, particularly security.

Thus, we propose a more detailed smart campus architectural framework that combines IoT and blockchain technology, as shown in Figure 2. Our smart campus framework consists of the blockchain and six layers:

1. **physical**, which includes several objects, such as campus sensors and devices;
2. **communication**, which includes the communication protocols and IoT gateway;
3. **platform**, which is a cloud component since it is recently considered an ideal technique for storing and analysing of volume of data as well as for running several services;
4. **data**, which is used to store campus data and includes real-time events;
5. **business**, which produces high-level reports and analysis; and
6. **application**, which provides services to the end user for connecting and controlling the smart campus environment.

In addition, this framework has a security system to provide a secure data connection that ensures the secure transfer of trusted data from the physical, communication, platform, data, business, to the final application layer.

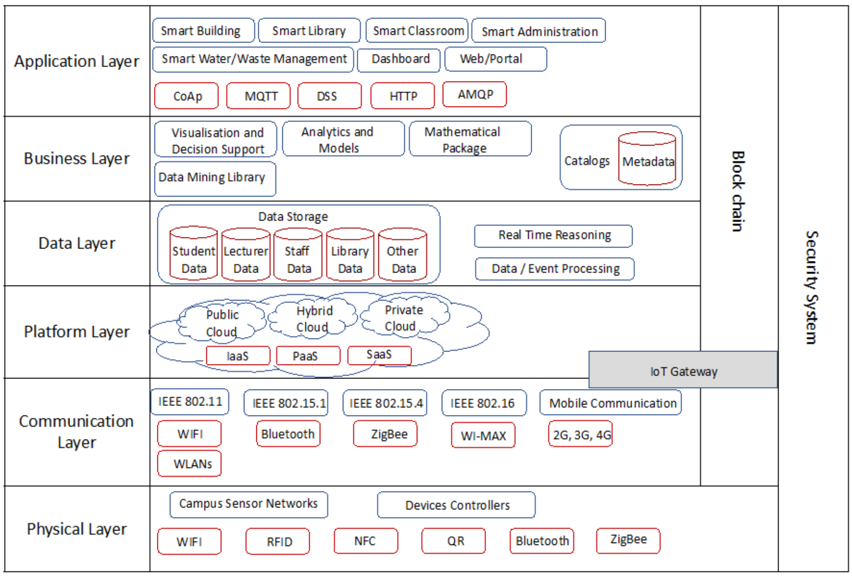

Fig. 2. A new smart campus framework

The following sub-sections describe each layer in more detail.

4.1 Physical Layer

The first layer, the physical layer, includes devices and sensors to detect data, such as motion, temperature, humidity, locations, attendance in the physical environment, etc. When the sensors sense the physical campus environment the parameters are then converted to data signals to be handled on the Cloud for analysing. On the way, such data may pass through brokerage protocols, such as MQTT, to a suitable blockchain-based distributed storage in the data layer. In the physical layer, actuators operate in the opposite way: they convert data signals into physical actions [58] perhaps as a response to sensor data stored on the blockchain, which is subsequently analysed and results in an actuator event. The devices in this layer represent hardware components that are connected to the upper layers of the architecture either wirelessly or by wires.

4.2 Communication Layer

The communication layer is sometimes known as the network layer or transmission layer [59, 60]. The different data sources that are provided by the perception layer need to be connected to the upper architecture layers to handle collected data. Devices and sensors use protocols and adequate communication technology to connect to the Internet. The diverse data sources in a smart environment lead to diverse communication technologies. For example, Wi-Fi/IEEE 802.11 utilises radio waves to allow smart devices to exchange and communicate within a 100 m range and without utilising a router in some *ad hoc* configurations [61]. IEEE 802.15.4 standard uses short-wavelength radio to exchange data between smart devices and to minimise power, such as Bluetooth low energy (BLE), which operates for a longer period of time and within a 100 m range. Recently, BLE was considered a suitable technology to support IoT applications [62]. In addition, IEEE 802.15.4 protocol is the specification of low high-message throughput, low cost, low data rate, and low power consumption and is also a good candidate for machine-to-machine (M2M), wireless sensor network, and IoT. This standard is used to produce Zigbee protocol for more reliable communication and a high level of security [61]. Therefore, the main objectives of this layer are to transmit data from and to different objects through gateways to integrated networks.

Biswas and Muthukkumarasamy [63] discussed using blockchain in a smart city to provide a secure communication platform. They illustrated that blockchain should be integrated with the network layer to provide privacy and the security of transmitted data. They recommended that the transaction data can be into blocks using TeleHash protocol for broadcast in the network.

4.3 Platform Layer

Generally, a smart environment based on IoT uses a large number of data sources, including actuators and sensors that produce big data, which need to extract knowledge by using complex computations, applying data mining algorithms, and managing the services and allocation tasks [64]. Thus, cloud computing presents the suitable technology and a powerful computational resource for IoT to process, compute, and store big data. In addition, blockchain is used to eliminate a centralised system architecture.

4.4 Data Layer

The data layer represents a database for the system and processing of the data. A huge amount of data is stored in this layer, which is called 'big data'. The previous layer uses this layer to generate useful information. In the case of a smart campus, blockchain with a decentralised structure is needed to add security and privacy to the data.

4.5 Business Layer

The business layer relies on middleware technology, which manages the system services and activities. It is responsible for building flowcharts, graphs, and business models as well as analysing, monitoring, evaluating, designing, and developing smart systems. Based on big data analysis, the business layer has the ability to support processing in decision making, visualise the outcomes to the user, and operate the controlling actuators.

4.6 Application Layer

This layer can consist of many different application types and services required by many different end users. For example, in a smart campus, this layer can provide data related to air humidity and temperature measurements. Therefore, the application layer's main objectives are to provide high-quality intelligent services to stockholders [65, 66] and allow users to interact with the system and visualise the data via an interface.

In addition, the application layer has some protocols to deal with. For instance:

- Constrained Application Protocol (CoAP) is one-to-one communication protocol that is inspired by Hypertext Transfer Protocol (HTTP).
  - CoAp is suitable for smart devices and IoT technology because CoAp is thin, lightweight, and causes as little traffic as possible [58].
- Message Queue Telemetry Transport (MQTT) is a protocol for messaging, and it is responsible for connecting networks and smart devices with middleware and applications [61]. Several applications use the MQTT, such as monitoring and social media notifications [58]. Thus, this protocol is able to provide an ideal messaging protocol for M2M and IoT communications due to its low bandwidth networks, low power, and low cost.
- Moreover, Advanced Message Queuing Protocol (AMQP) is an open standard protocol that supports reliable transport protocol and communication and focuses on a message-oriented environment. Data Distribution Service (DDS) is a publish–subscribe protocol for real-time communication [65].

The application layer is responsible for providing high reliability and excellent quality of service to the applications. Therefore, there are a variety of communication protocols that can each work in a different scenario and with a different device manufacturer.

4.7 Blockchain

Blockchain is a distributed ledger technology that implements transactions with a decentralised digital database. The transaction is verified by a network of computers before it is added and updated to the ledger. Blockchain allows parties to exchange assets in real time without going through intermediaries [67]. Blockchain technology is a peer-to-peer (P2P) distributed ledger technology that records contracts, transactions, and agreements [63, 68]. In other words, blockchain verifies data after receiving it from a physical layer then constructs it into a transaction. It should be stated that the details of blockchain technology and how it works are outside the scope of this paper. For more information about blockchain technology principles, [69] and [70] can be helpful. To decide which type of blockchain to use in our framework, the types will be addressed in a comparative analysis.

Recently, blockchain technology has been classified into three types: public blockchain, private blockchain, and consortium blockchain [71]. The first type is also called a permission-less blockchain because there is no need for permission for a single entity, such as Bitcoin [72] or Ethereum [73], to join the network. Anyone can engage and participate successfully by downloading the blockchain and executing the code as well as by sending transactions to the network. Therefore, a public blockchain is fully decentralised so all transactions or ledgers are shared and verified by all nodes, and there is no need for a central authority. In order to prove identities, peers in networks have to solve the proof-of-work puzzle, which requires time and power. This means the chain is not centralised, and once the data is validated the ledger is changed; therefore, the ledger or the transaction is immutable.

However, a private blockchain is designated by its participants in advance to allow it writing, reading, and consensus processes. In other words, this blockchain is a permission-based chain, and only those who are authorised can join the network. This type of blockchain is useful for organisations or groups of individuals that share the ledger privately. Thus, malicious nodes cannot enter the network without permission. Specific nodes or services can be removed or added as needed, which provides better scalability for the network. Since the private blockchain is controlled on the network by a single trust node and has fewer authorised participants than a public blockchain, it performs much faster on a ledger and processes more transactions for each block. Furthermore, this blockchain has many consensus methods, such as practical Byzantine fault tolerance, proof of elapsed time, and proof of stake. A private blockchain is used widely in an environment that needs more security and privacy, such as by companies and in the banking sector. Cordra [74] is an example of a private blockchain.

In addition, a consortium blockchain is a hybrid that combines private and public blockchains, and it is classified as a permission-based blockchain [71]. In this blockchain, the participants engage in writing and reading on the blockchain across organisations. The preselected nodes control the consensus process in this blockchain. In other words, several institutions govern this blockchain, unlike a private blockchain, which is operated by a single node. A hybrid blockchain has many advantages that relate to a private blockchain, such as privacy and efficiency of the ledger as well as higher scalability and faster transactions. In addition, a consortium blockchain is an easily implemented environment and more energy-efficient compared to a public blockchain [71, 75].

To summarise, all blockchain types are decentralised P2P networks, and all nodes share a verified ledger. All blockchains provide a ledger's immutability. All users in all types of blockchain maintain a replica of the ledger. However, the main difference between public and private blockchain is authorisation. A public blockchain allows any users to participate in the network.

In addition, private and consortium blockchains are more efficient for IoT networks since they both have faster response times in the network and lower computational requirements. While public blockchain has proved over the years to be suitable and efficient for cryptocurrencies, it is not that effective to use for IoT applications due to its bandwidth requirements and high computational requirements [76].

In our architecture, we suggest using a consortium blockchain, for example, the Hyperledger Fabric blockchain platform [77–79], for many key features. A Hyperledger blockchain is widely used for businesses and enterprises. It is designed to support pluggable implementation of components delivering high degrees of confidentiality, resilience, scalability, and low latency. Hyperledger has a modular architecture and can be used very flexibly. In addition, modular consensus protocols are been used, which permit a user to trust models and tailor the system for particular use cases. This platform runs smart contracts or chain code, which is an executing programmable code that allows participants to write their own scripts without a middleman [80].

5 Smart Campus Exploiting the Internet of Things, Blockchain, and Security Requirements

The main reason for developing a blockchain in 2008 was to address the potential problem related to stakeholders' trust in various use cases, including financial and non-financial fields [81, 82]. It provides security requirements for the transactions by using several cryptography mechanisms, such as signature, asymmetric cryptography, and hash. A lot of research has explored whether blockchain technology meets the need for providing more secure, trusted, and immutable data by adopting the blockchain into existing software, such as in the financial industry [83] and healthcare fields [84–86]. However, integrating blockchain technology into education institutions is still in its early stages and needs more research. We have therefore provided a discussion about security requirements for the proposed framework of a smart campus since the security aspect is the main concern in most of the recent blockchain applications. We would like to study this aspect in more detail in the following sub-sections, covering authorisation and privacy in addition to the CIA triad of confidentiality, integrity, and availability.

5.1 Authentication

Authentication is one of the key security aspects and is a process of verifying a peer's identity in order to use a system and communicate with each other [87]. There are many studies that have focused on user authentication with the majority of cases looking at data leaks and identity theft. The current authentication mechanisms, which have been used in most applications, vary from using a single factor, for example, a password or user ID, to using a multi-factor authentication, such as a smart card or biological characteristic. These traditional methods are not effective in providing appropriate protection and can cause various issues and damage, for example, recently passwords have been easily and frequently hacked [88]. Multi-factor authentication relies on centralisation or trusting third-party services, which, as we discussed previously, have high security risks.

Recently blockchain has been used to improve protection against illegitimate access of several IoT applications without the need for centralised services. For example, Cha et al. [89] designed a blockchain gateway by integrating the blockchain in an IoT gateway to securely protect user preferences while connecting to IoT devices. This approach can raise the authentication level between the users and the connected devices. In addition, Sanda and Inaba [90] used blockchain technology with a Wi-Fi network to provide the authentication to the connected users and protect the network from malicious usage. The blockchain in this implementation was used to encrypt the communication and ensure security to the network. Therefore, the blockchain has the benefit of increasing the security of the authentication aspects.

5.2 Privacy

Privacy is an essential aspect for most of the systems. The majority of the researchers have taken advantage of blockchain technology to increase the level of privacy in the IoT environment and protect the individual private data being revealed [91]. For example, Kianmajd et al. [92] presented a framework that integrates blockchain to preserve users' privacy while using community resources. The framework highlighted that the decentralised environment of the blockchain can be used to increase the users' data privacy. In addition, Zyskind et al. [93] structured a personal data management platform in order to provide privacy for users. The study proposed a protocol that integrated with a blockchain to produce 'an automated trustless access-control manager'. The constructed platform achieved the privacy using encrypted data in the ledger and storing pointers to it instead of the transaction of the data itself to the network. Thus, personal data should be secured and controlled by the user and not be trusted to a third party.

5.3 Confidentiality, Integrity, and Availability (CIA)

Data confidentiality is an aspect of protecting data from unauthorised access. Since blockchain uses cryptography mechanisms, it offers confidentiality and protects data, such as bank account [81] and personal data [94], from parties that do not have permission.

Data integrity is another security aspect that is concerned with assuring and preserving the consistency, reliability, and accuracy of the data [95]. In other words, the data stored in the database should be kept from changing throughout its lifecycle. In this case, through the use of various cryptography mechanisms, blockchain technology provides data integrity and promises to protect data from unauthorised change [96, 97]. Banerjee et al. [98] combined the blockchain with IoT devices' firmware to maintain the integrity of shared data. Moreover, Liu et al. [99] implemented a framework for a data integrity service using blockchain to verify the integrity of IoT data without the need for a third party.

Data availability is one of many important terms in any system and means ensuring that the required data is available and accessible when needed [100]. One of the benefits of blockchain technology with a decentralised structure and distributed ledger is that it is resistant to outages [101].

6 Conclusion

Recently, many researchers have focused on the study of developing smart and intelligent environments in many fields, such as smart cities, hospitals, and homes that mostly rely on IoT systems. The privacy and security aspects have been attracting research interest since they are considered the critical issues and challenges for connected IoT devices. This paper surveyed a number of schemes and frameworks for smart campuses that were proposed in the literature as an example of IoT and addressed the issues related to security and privacy.

This paper presented an overview of the smart campus concept, including architectures; enabling different technologies, such as IoT; cloud computing; and blockchain with the aim of improving the quality of life on campuses. It studied eight varied domains in the smart campus and defined problem assets per domain. In addition, the paper discussed the generic framework of a smart campus and its limitations. Furthermore, we proposed a new smart campus framework combining IoT and blockchain to mitigate the IoT issues in the previous architectures, particularly in relation to security and privacy since blockchain technology has multiple properties, such as autonomous and decentralised control, support for integrity, and resiliency. Moreover, this study discussed the security requirements for the proposed framework of a smart campus.

References

1. Kwok, L.: A vision for the development of i-campus. Smart Learn. Environ. 2, 2 (2015).
2. Szabo, R., Farkas, K., Ispany, M., Benczur, A.A., Batfai, N., Jeszenszky, P., Laki, S., Vagner, A., Kollar, L., Sidlo, C., Besenczi, R., Smajda, M., Kover, G., Szincsak, T., Kadek, T., Kosa, M., Adamko, A., Lendak, I., Wiandt, B., Tomas, T., Nagy, A.Z., Feher, G.: Framework for smart city applications based on participatory sensing. In: 4th IEEE International Conference on Cognitive Infocommunications, CogInfoCom 2013 - Proceedings. pp. 295–300 (2013).
3. Caragliu, A., Bo, C. Del, Nijkamp, P.: Smart Cities in Europe Smart Cities in Europe. 3rd Cent. Eur. Conf. Reg. Sci. 0732, 1–15 (2015).
4. Perera, C., Liu, C.H., Jayawardena, S., Chen, M.: A Survey on Internet of Things from Industrial Market Perspective. IEEE Access. 2, 1660–1679 (2015).
5. Pramanik, M.I., Lau, R.Y.K., Demirkan, H., Azad, M.A.K.: Smart health: Big data enabled health paradigm within smart cities, (2017).
6. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M.L., Tarricone, L.: An IoT-Aware Architecture for Smart Healthcare Systems. IEEE Internet Things J. (2015).
7. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., Mankodiya, K.: Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Futur. Gener. Comput. Syst. (2018).
8. Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., Marrocco, G.: RFID technology for IoT-based personal healthcare in smart spaces. IEEE Internet Things J. (2014).
9. Tachizawa, E.M., Alvarez-Gil, M.J., Montes-Sancho, M.J.: How “smart cities” will change supply chain management. Supply Chain Manag. (2015).
10. Lukić, J., Radenković, M., Despotović-Zrakić, M., Labus, A., Bogdanović, Z.: Supply chain intelligence for electricity markets: A smart grid perspective. Inf. Syst. Front. (2017).
11. Ghazal, B., Elkhatib, K., Chahine, K., Kherfan, M.: Smart traffic light control system. In: 2016 3rd International Conference on Electrical, Electronics, Computer Engineering and their Applications, EECEA 2016 (2016).
12. Galán-García, J.L., Aguilera-Venegas, G., Rodríguez-Cielos, P.: An accelerated-time simulation for traffic flow in a smart city. J. Comput. Appl. Math. (2014).
13. Nair, P.K., Ali, F., Lim, C.L.: Interactive Technology and Smart Education Article information : Interact. Technol. Smart Educ. (2015).
14. Alelaiwi, A., Alghamdi, A., Shorfuzzaman, M., Rawashdeh, M., Hossain, M.S., Muhammad, G.: Enhanced engineering education using smart class environment. Comput. Human Behav. (2015).
15. Ibrahim, M.S., Razak, A.Z.A., Kenayathulla, H.B.: Smart Principals and Smart Schools. Procedia - Soc. Behav. Sci. (2013).
16. Muhamad, W., Kurniawan, N.B., Suhardi, S., Yazid, S.: Smart campus features, technologies, and applications: A systematic literature review. In: 2017 International Conference on Information Technology Systems and Innovation, ICITSI 2017 - Proceedings (2018).
17. Dong, X., Kong, X., Zhang, F., Chen, Z., Kang, J.: OnCampus: a mobile platform towards a smart campus Background. Springerplus. 5, (2016).
18. Ahern, N., Wink, D.M.: Virtual learning environments: Second life. Nurse Educ. (2010).
19. Alam, A., Ullah, S.: Adaptive 3D-Virtual Learning Environments: From Students' Learning Perspective. In: Proceedings - 14th International Conference on Frontiers of Information Technology, FIT 2016 (2017).

20. Komaki, H., Shimazaki, S., Sakakibara, K., Matsumoto, T.: Interactive optimization techniques based on a column generation model for timetabling problems of university makeup courses. In: 2015 IEEE 8th International Workshop on Computational Intelligence and Applications, IWCIA 2015 - Proceedings (2016).
21. Mei, R., Guan, J., Li, B.: University course timetable system design and implementation based on mathematical model. In: 2010 The 2nd International Conference on Computer and Automation Engineering, ICCAE 2010 (2010).
22. Abuarqoub, A., Abusaimeh, H., Hammoudeh, M., Uliyan, D., Abu-Hashem, M.A., Murad, S., Al-Jarrah, M., Al-Fayez, F.: A Survey on Internet of Thing Enabled Smart Campus Applications. Proc. Int. Conf. Futur. Networks Distrib. Syst. - ICFNDS '17. 1–7 (2017).
23. Khamayseh, Y., Mardini, W., Aljawarneh, S., Yassein, M.B.: Integration of Wireless Technologies in Smart University Campus Environment. Int. J. Inf. Commun. Technol. Educ. 11, 60–74 (2015).
24. Atif, Y., Mathew, S.S., Lakas, A.: Building a smart campus to support ubiquitous learning. J. Ambient Intell. Humaniz. Comput. 6, 223–238 (2015).
25. Chen, Y., Zhang, R., Shang, X., Zhang, S.: An intelligent campus space model based on the service encapsulation. In: LISS 2012 - Proceedings of 2nd International Conference on Logistics, Informatics and Service Science. pp. 919–923 (2013).
26. Chen, Y., Li, X., Wang, Y., Gao, L.: The design and implementation of intelligent campus security tracking system based on RFID and ZigBee. In: 2011 2nd International Conference on Mechanic Automation and Control Engineering, MACE 2011 - Proceedings. pp. 1749–1752 (2011).
27. Ng, J.W.P., Azarmi, N., Leida, M., Saffre, F., Afzal, A., Yoo, P.D.: The intelligent campus (iCampus): End-to-end learning lifecycle of a knowledge ecosystem. In: Proceedings - 2010 6th International Conference on Intelligent Environments, IE 2010. pp. 332–337 (2010).
28. Jackson, P.M.: Intelligent campus. In: SPCA 2006: 2006 First International Symposium on Pervasive Computing and Applications, Proceedings. p. 3 (2007).
29. Hirsch, B., Ng, J.W.P.: Education beyond the cloud: Anytime-anywhere learning in a smart campus environment. 2011 Int. Conf. Internet Technol. Secur. Trans. 718–723 (2011).
30. Atif, Y., Mathew, S.: A social web of things approach to a smart campus model. In: Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-iThings-CPSCom 2013. pp. 349–354 (2013).
31. Liu, Y.L., Zhang, W.H., Dong, P.: Research on the Construction of Smart Campus Based on the Internet of Things and Cloud Computing. Appl. Mech. Mater. (2014).
32. Adamkó, A., Kollár, L.: A system model and applications for intelligent campuses. In: INES 2014 - IEEE 18th International Conference on Intelligent Engineering Systems, Proceedings. pp. 193–198 (2014).
33. Boran, A., Bedini, I., Matheus, C.J., Patel-Schneider, P.F., Keeney, J.: A smart campus prototype for demonstrating the semantic integration of heterogeneous data. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 238–243 (2011).
34. Yu, Z., Liang, Y., Xu, B., Yang, Y., Guo, B.: Towards a smart campus with mobile social networking. In: Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011 (2011).

35. De Angelis, E., Ciribini, A.L.C., Tagliabue, L.C., Paneroni, M.: The Brescia Smart Campus Demonstrator. Renovation toward a zero Energy Classroom Building. In: Procedia Engineering. pp. 735–743 (2015).
36. Kolokotsa, D., Gobakis, K., Papantoniou, S., Georgatou, C., Kampelis, N., Kalaitzakis, K., Vasilakopoulou, K., Santamouris, M.: Development of a web based energy management system for University Campuses: The CAMP-IT platform. Energy Build. 123, 119–135 (2016).
37. Han, Y., Xia, K.: Data preprocessing method based on user characteristic of interests for web log mining. In: Proceedings - 2014 4th International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2014. pp. 867–872 (2014).
38. Kuang, W., Luo, N.: User interests mining based on topic map. In: Proceedings - 2010 7th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2010. pp. 2399–2402 (2010).
39. Amr, A.I., Kamel, S., Gohary, G. El, Hamhaber, J.: Water as an Ecological Factor for a Sustainable Campus Landscape. Procedia - Soc. Behav. Sci. 216, 181–193 (2016).
40. Shi, G.B.: The design of campus monitoring and managing system for watersaving based on webgis. Proc. - 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017. 2018–Janua, 951–954 (2018).
41. Kudva, V.D., Nayak, P., Rawat, A., Anjana, G.R., Kumar, K.R.S., Amrutur, B., Kumar, M.S.M.: Towards a Real-Time Campus-Scale Water Balance Monitoring System. In: Proceedings of the IEEE International Conference on VLSI Design. pp. 87–92 (2015).
42. Verma, P., Kumar, A., Rathod, N., Jain, P., Mallikarjun, S., Subramanian, R., Amrutur, B., Kumar, M.S.M., Sundaresan, R.: Towards an IoT based water management system for a campus. In: 2015 IEEE 1st International Smart Cities Conference, ISC2 2015 (2015).
43. Alghamdi, A., Shetty, S.: Survey toward a smart campus using the internet of things. In: Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016. pp. 235–239 (2016).
44. Mudumbe, M.J., Abu-Mahfouz, A.M.: Smart water meter system for user-centric consumption measurement. In: Proceeding - 2015 IEEE International Conference on Industrial Informatics, INDIN 2015. pp. 993–998 (2015).
45. Goenka, S., Mangrulkar, R.S.: Robust Waste Collection: Exploiting IOT Potentiality in Smart Cities. i-Manager's J. Softw. Eng. 11, 10–18 (2017).
46. Folianto, F., Low, Y.S., Yeow, W.L.: Smartbin: Smart waste management system. In: 2015 IEEE 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2015 (2015).
47. Ebrahimi, K., North, L., Yan, J.: GIS applications in developing zero-waste strategies at a mid-size American university. In: International Conference on Geoinformatics (2017).
48. Saad, S.A., Hisham, A.A.B., Ishak, M.H.I., Fauzi, M.H.M., Baharudin, M.A., Idris, N.H.: Real-time on-campus public transportation monitoring system. In: Proceedings - 2018 IEEE 14th International Colloquium on Signal Processing and its Application, CSPA 2018 (2018).
49. Ramadan, M., Al-Khedher, M., Al-Kheder, S.: Intelligent anti-theft and tracking system for automobiles. Int. J. Mach. Learn. Comput. (2012).
50. Priya, S., Prabhavathi, B., Shanmuga Priya, P., Shanthini, B., Scholar, U.: An Android Application for Tracking College Bus Using Google Map. Int. J. Comput. Sci. Eng. Commun. (2015).

51. Suresh Mane, M.P., Khairnar, P.V.: Analysis of Bus Tracking System Using Gps on Smart Phones. IOSR J. Comput. Eng. (2014).
52. Ferreira, J.E., Visintin, J.A., Okamoto, J., Pu, C.: Smart services: A case study on smarter public safety by a mobile app for University of São Paulo. 2017 IEEE SmartWorld Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People Smart City Innov. SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI 2017 - . 1–5 (2018).
53. Wang, Y., Saez, B., Szczechowicz, J., Ruisi, J., Kraft, T., Toscano, S., Vacco, Z., Nicolas, K.: A smart campus internet of things framework. In: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017 (2018).
54. Cheng, X., Xue, R.: Construction of Smart Campus System Based on Cloud Computing. Presented at the (2016).
55. Atlam, H.F., Wills, G.B.: Intersections between IoT and distributed ledger, (2019).
56. Halpin, H., Piekarska, M.: Introduction to security and privacy on the blockchain. In: Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017 (2017).
57. Chowdhury, M., Ferdous, S., Biswas, K.: Blockchain Platforms for IoT Use-cases. 3–4 (2018).
58. Hejazi, H., Rajab, H., Cinkler, T., Lengyel, L.: Survey of platforms for massive IoT. In: 2018 IEEE International Conference on Future IoT Technologies, Future IoT 2018 (2018).
59. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet Things J. (2017).
60. Leo, M., Battisti, F., Carli, M., Neri, A.: A federated architecture approach for Internet of Things security. In: 2014 Euro Med Telco Conference - From Network Infrastructures to Network Fabric: Revolution at the Edges, EMTC 2014 (2014).
61. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutorials. (2015).
62. Decuir, J.: Introducing bluetooth smart: Part 1: A look at both classic and new technologies, (2014).
63. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016 (2017).
64. Bryant, R., Katz, R., Lazowska, E.: Big-Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society. Comput. Res. Assoc. (2008).
65. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: The internet of things architecture, possible applications and key challenges. In: Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012 (2012).
66. Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., Liu, W.: Study and application on the architecture and key technologies for IOT. In: 2011 International Conference on Multimedia Technology, ICMT 2011 (2011).
67. Morkunas, V.J., Paschen, J., Boon, E.: How blockchain technologies impact your business model. Bus. Horiz. 2018, (2019).
68. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things, (2016).

69. Olleros, F., Zhegu, M., Pilkington, M.: Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations (2016).
70. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: Blockchain technology innovations. In: 2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017 (2017).
71. Sankar, L.S., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. In: 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017 (2017).
72. Satoshi, N., Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic cash system. Bitcoin. (2008).
73. Dannen, C.: Introducing ethereum and solidity: Foundations of cryptocurrency and blockchain programming for beginners. (2017).
74. Hearn, M.: Corda: A distributed ledger. Whitepaper. (2016).
75. Lim, S.Y., Tankam Fotsing, P., Almasri, A., Musa, O., Mat Kiah, M.L., Ang, T.F., Ismail, R.: Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. Int. J. Adv. Sci. Eng. Inf. Technol. (2018).
76. Salimitari, M., Chatterjee, M.: A Survey on Consensus Protocols in Blockchain for IoT Networks. 1–15 (2018).
77. Windley, P.J.: Hyperledger Welcomes Project Indy. Hyperledger. (2017).
78. Cachin, C.: Architecture of the Hyperledger Blockchain Fabric. Work. Distrib. Cryptocurrencies Consens. Ledgers (DCCL 2016). (2016).
79. Androulaki, E., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Barger, A., Cocco, S.W., Yellick, J., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G.: Hyperledger fabric. Presented at the (2018).
80. Buterin, V., Abarbanell, J.S., Bushee, B.J., Adcock, C., Adebiyi, A.A., Adewumi, A.O., Ayo, C.K., Atzei, N., B, M.B., Cimoli, T., Bartoletti, M., Cimoli, T., B, Y.H., Chakraborty, K., Mehrotra, K., Mohan, C.K., Ranka, S., Chen, M., Narwal, N., Schultz, M., Choi, H.K., Choudhry, R., Garg, K., Chrystus, J., Connor, J.T., Martin, R.D., Atlas, L.E., Corbet, S., Lucey, B., Yarovaya, L., Dechow, P.M., Hutton, A.P., Meulbroek, L.K., Sloan, R.G., Duarte Lima Freire Lopes, G., Falinouss, P., Faugeras, O.D., Fischer, T., Krauss, C., Frisiani, N., Hebrero-Martínez, M., Lerma, R.V., Trollé, C.M., Pérez-Cuevas, R., Muñoz, O., Hu, Z., Liu, W., Bian, J., Liu, X., Liu, T.-Y., Kadiri, E., Alabi, O., Kim, Y. Bin, Kim, J.G.J.H., Kim, W., Im, J.H., Kim, T.H., Kang, S.J., Kim, C.H., Lee, J., Park, N., Choo, J., Kim, J.G.J.H., Kim, C.H., Kimoto, T., Asakawa, K., Yoda, M., Takeoka, M., Kohara, K., LeCun, Y., Bengio, Y., Maciel, L.S., Ballini, R., Mu, S., Guo, Y., Yang, P., Wang, W., Yu, L., Nelson, D.M.Q., Pereira, A.C.M., De Oliveira, R.A., Of, a B., Counsel, P., Pagolu, V.S., Reddy, K.N., Panda, G., Majhi, B., Persson, S., Shaw, I., Phaladisailoed, T., Numnonda, T., Richardson, S., Tuna, I., Wysocki, P., Roche, J., Mcnally, S., Roondiwala, M., Patel, H. and Varma, S., Shukla, N., Fricklas, K., Song, Y.-G., Zhou, Y.-L., Han, R.-J., Tang, Z., de Almeida, C., Fishwick, P.A., Vargas, M.R., Lima, B.S.L.P. De, Evsukoff, A.G., Chohan, U., Nakamoto, S., Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., Hess, J., Wiederhold, B.K., Riva, G., Graffigna, G., Schöneburg, E., Guo, T., Bifet, A., Antulov-Fantulin, N., Wood, G., Vineeth, N., Ayyappa, M., Bharathi, B.: A next-generation smart contract and decentralized application platform. PLoS One. (2018).
81. Crosby, M., Nachiappan, Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain Technology - BEYOND BITCOIN. Berkley Eng. (2016).
82. Davidson, S., De Filippi, P., Potts, J.: Economics of Blockchain. SSRN Electron. J. (2016).

83. Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., Thompson, C.: A Distributed-Ledger Consortium Model for Collaborative Innovation. Computer (Long. Beach. Calif). (2017).
84. Benchoufi, M., Porcher, R., Ravaud, P.: Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research. (2018).
85. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: MedRec: Using blockchain for medical data access and permission management. In: Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016 (2016).
86. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. (2018).
87. Wazid, M., Das, A.K., Hussain, R., Succi, G., Rodrigues, J.J.P.C.: Authentication in cloud-driven IoT-based big data environment: Survey and outlook. J. Syst. Archit. (2019).
88. Mhenni, A., Cherrier, E., Rosenberger, C., Essoukri Ben Amara, N.: Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. Comput. Secur. (2019).
89. Cha, S.C., Chen, J.F., Su, C., Yeh, K.H.: A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things. IEEE Access. (2018).
90. Sanda, T., Inaba, H.: Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0. In: 2016 IEEE 5th Global Conference on Consumer Electronics, GCCE 2016 (2016).
91. Mohsin, A.H., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Albahri, A.S., Alsalem, M.A., Mohammed, K.I.: Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions, (2019).
92. Kianmajd, P., Rowe, J., Levitt, K.: Privacy-preserving coordination for smart communities. In: Proceedings - IEEE INFOCOM (2016).
93. Zyskind, G., Nathan, O., Pentland, A.S.: Decentralizing privacy: Using blockchain to protect personal data. In: Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015 (2015).
94. Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K.: A Blockchain-Based Approach to Health Information Exchange Networks. Proc. NIST Work. Blockchain Healthc. (2016).
95. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., Imran, M.: Securing IoTs in distributed blockchain: Analysis, requirements and open issues. Futur. Gener. Comput. Syst. (2019).
96. Wüst, K., Gervais, A.: Do you need a Blockchain? IACR Cryptol. ePrint Arch. (2017).
97. Apte, S., Petrovsky, N.: Will blockchain technology revolutionize excipient supply chain management?, (2016).
98. Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for internet of things security: a position paper. Digit. Commun. Networks. (2018).
99. Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L.: Blockchain Based Data Integrity Service Framework for IoT Data. In: Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017 (2017).
100. Scarfone, K., Tracy, M.: Guide to General Server Security. Natl. Inst. Stand. Technol. (2008).
101. Zhu, H., Zhou, Z.Z.: Analysis and outlook of applications of blockchain technology to equity crowdfunding in China, (2016).